PIJSSL

Praxis International Journal of Social Science and Literature

A Peer-reviewed Multidisciplinary e-Journal with SJIR 2025 = 6.034 & ISSN: 2581-6675

Vol. 09, No. 01 (January 2026) **DOI:** 10.51879/PIJSSL/090107

Email: editor.pijssl@gmail.com | **Website:** www.pijssl.com

OPEN ACCESS

Revisiting US Realism in age of Hybrid Threat: Integrating Cyber, AI and Information in National Security Strategy

Yash Seela

PhD Scholar, Centre for the Study of the Americas, School of International Studies, Jawaharlal Nehru University, New Delhi. Email: yashseela016@gmail.com

Abstract

Emergence of hybrid threats is unprecedented phenomena in recent years. Various theoretical frameworks are employed to get cognisance of this new form of threat. Many scholars of the rupture theisis argue that existing realist theory cannot explain emerging cyber threats in virtual world in terms of power struggle, coercion, force etc. Therefore, the purpose of this study is to investigate whether the realist theory in United States can explain hybrid warfare in context of cyber, Artificial Intelligence and information. By analyzing the security policy documents of United States, the study asserts that hybrid threat and policy response of United States still exhibits the realist tradition by using the phrases and words like "dominant force", "deterring aggression" and "defending forward". Two case studies of OPM data breach and US Cyber Command also help to understand the hybrid threat further from realist lenses.

Keywords: *Hybrid Threat, Realism, Cyber, Information, Artificial Intelligence, Defending Forward.*

Introduction

Hybrid warfare is in contrast with military centric conventional warfare as fought traditionally. Conventional warfare is conducted by regular, uniformed, and national military units and uses conventional military weapons and battlefield techniques. Johann Schmid (2012) defines hybrid warfare as "creative act of force combining a broad spectrum of military and non-military instruments and vectors of power on an extended multi- domain battlespace, ranging from politics, diplomacy, information, economy, technology, military and society to dimensions like culture, psychology, legitimacy and morale, while ambiguously operating in the shadow/grey-zones of blurred interfaces between war and peace, friend and foe, internal and external relations, civil and military as well as state and non-state actors and fields of responsibilities with the ultimate goal to enable an own decision of the confrontation primarily on non-military centers of gravity while preventing being militarily overthrown or compelled by the enemy".

The definition captures the full spectrum of nature of contemporary conflict by inclusion of politics, economy, diplomacy, information, military society, and culture. Thus, making it more realistic than traditional military centric definition. However, calling it "creative act of force" is rhetorically impressive but analytically vague as creativity in warfare varies and difficult to systematise.

During the past few years, various regions including America brought up such issues named "hybrid threats" - these threats are combined in various ways like cyber-operations, information warfare/disinformation, economic coercion, AI-enabled tools, diplomacy, and so on. These are different ways and sources of power. But still, on a deeper level, state behavior is about power, security, survival, and relative advantages. So, the question is: Are these hybrid capabilities indicating a discontinuity with the

This is an open access article licensed under https://creativecommons.org/licenses/by-nc-nd/4.0

traditional realist logic of state behavior, or are they merely new instruments with which the same logic is being enacted?

According to Filipec (2019), modern hybrid warfare should be understood in the context of the already existing theoretical traditions - Realism, Liberalism, and Constructivism. This is because each of these theories helps us to understand different aspects of the practice: realism shows the power-political logic of the conflict, liberalism, regime-based goals, and constructivism, the manipulation of identities and norms. However, it is still challenging to define hybrid warfare, as the term is now used to describe a wide range of actors and means, such as special forces, intelligence operatives, cyber operations, disinformation, and electronic warfare, among others.

In such a context, this study claims that adding cyber, artificial intelligence, and information-domain tools to the U.S. national security strategy is a change of the adaptation to the already existing realist traditions - not a rupture. Although the technological elements of war have changed drastically, the underlying strategic logic of power maximization, threat perception, deterrence, and relative gains is still in line with the core ideas of classical, structural, and neoclassical realism.

To evaluate this statement in a complete manner, the article examines two sets of questions:

RQ1: How can current realist theories explain the incorporation of cyber, AI, and information capabilities in the U.S. national security strategy documents?

RQ2: To what extent do U.S. strategic doctrines and operational behaviors manifest continuance of realist principles when dealing with hybrid threats?

Answering these questions, the research tries to demonstrate that technological breakthrough changes how states exercise power, but not the basic logic of realist power politics.

Literature Review

Morgenthau (1949) insisted that any instrument be military, economic, or otherwise should be evaluated in terms of contribution to national power. This insight also applies to emerging domain such as cyber and AI, which the U.S. increasingly treats as strategic assets within a realist power framework. Hybrid threats are essentially silent fights happening below the level of traditional war. They are usually a challenge in the mind rather than a military battle. Since hybrid activities for the most part steer clear of open warfare and are still psychological conflicts, they are clearly in line with Morgenthau's concept of political power as the ability to affect rather than use force. Realism also sees through the veil to explain why states combine hybrid measures with their traditional ones: in a situation where a military action is expensive or limited by the geographical features, technology, or lack of resources, states use different instruments of power. In this way, hybrid warfare is a logical continuation of the use of state power which enables states to affect their adversaries without escalating the conflict and saving their resources.

Recent research is starting to look beyond the argument about treating the internet as just a new 'domain' of state operations. While one group considers cyber capabilities as something totally revolutionary (Arquilla & Ronfeldt, Nye), and the other group sees them as having only limited effects (Lindsay; Libicki; Valeriano & Maness), both views are still constrained by their domain-based assumptions. Foulon and Meibauer (2024) provide a major conceptual shift by suggesting that cyberspace acts as a structural modifier in international relations. It does not just facilitate cyber operations, but, according to the authors, cyberspace changes the way states 'experience anarchy, conduct intelligence, manage vulnerabilities, and interpret deterrence'. From this perspective, cyberspace changes the systemic environment in which states operate to gain power and ensure their security, thus changing the traditional dynamics of realist theory, but not substituting them. The present study's argument is very much in agreement with this, which is that U.S. cyber, AI, and information strategies are not departures from the realist theory but rather adaptations within it.

Edleman (2013) in his doctoral thesis identifies what he refers to "paradigm shift" thesis in the field of cyber studies - the idea that cyberattacks are a sudden break from traditional coercion; they replace kinetic power and are beyond existing international norms (pp. 127-128). He discards this contention by pointing out that electronic disruption has always been a part of statecraft and that cyber operations are not conceptually different from war, nor are they governed by existing laws and state practices (pp. 128-129). Therefore, Edelman agrees with those theorists of continuity who maintain that cyber means of warfare are just an evolution of the already existing strategic logics and not a radical change. Moreover, Edelman's criticism is in line with a wider academic agreement, which is reflected in the caution raised by most scholars not to exaggerate the newness of the cyber conflict. In his work, Rid (2013) gives the example of one such scholar when he explains that cyber operations are mostly traditional ones in the arena of political warfare, since they are performed as acts of sabotage, espionage, or subversion to a large extent and only rarely as a new type of violence (Rid, 2013). Through the placement of cyberattacks into these timeless strategic mechanisms, Edelman points out that the rationale of state behavior is still influenced by the age-old principles of coercion and competition. Consequently, his denial of the "paradigm shift" idea is in line with the continuity school's position that cyber conflict is not a break with the international political practice but the update of the existing means of statecraft.

Analytical framework: Realism and the hybrid threat

Morgenthau's point that unification through technology does not lead to moral unification anticipates the present-day information warfare. The hybrid threats use the same psychological mechanisms that Morgenthau describes 'information is processed through national experiences and interests, which makes disinformation, narrative warfare, and perception manipulation not only compatible but also the most effective ways of power strengthening rather than causes of global unification' (Morgenthau, 1949: 201-202).

From the perspective of structural realists, Morgenthau's argument is a demonstration that technological interconnectedness does not eliminate anarchy; instead, it deepens the strategic competition. Consequently, in order to deal with the cyber and AI-driven security dilemma, states are employing technologies in such a way that they restrict communication, censor information, monitor populations, and at the same time, gain relative informational advantage. These behaviors are very much in line with the security dilemma caused by cyber and AI, and are typical of today's world of cyber and AI-driven security dilemma.

When Morgenthau suggests that nations interpret the same facts differently, he is indirectly providing support for the neoclassical realist framework which emphasizes the influence of elite perception, strategic culture, and domestic politics. In the American case, the hybrid-threat strategy is processed through a technological ecosystem, intelligence bureaucracy, and political culture, which then gives rise to the unique form of cyber–AI–information integration. Morgenthau's deconstruction of technology as a unifying force predicts the very idea of modern hybrid threats. It is not that technology creates a common global public sphere, but rather that it deepens national cleavages and gives states the tools they need to shape, distort, or close off information flows. Hybrid warfare is a perfect example of how Morgenthau's points are still valid: the fragmented interpretations, state-controlled narratives, and the use of info as a strategic resource.

At this stage, neoclassical realism is the factor that clarifies the picture. It helps to focus not only on the pressures the system exerts but also on the way domestic institutions, technological-industrial capacity, and elite threat perceptions influence the process of converting the external pressures into specific national strategies. In such a situation, a neoclassical realist explanation of a kind that moves in the direction of Buchanan's argument concerning the U.S. home-field digital advantages basically, the dominance of American technology firms, the intelligence architecture of NSA and CYBERCOM, and elite perceptions of

China and Russia as revisionist digital competitors, seems very convincing comes in handy (Buchanan, 2020).

Every technological shift had forced the military to adapt without replacing the core logic of survival, competition, and deterrence. This argument holds true in the light of the Revolution in Military Affairs (RMA). Each technological transition from RMA I-industrial mechanization to RMA III-nuclear strategy and the digital–networked era (RMA IV) has broadened the set of instruments available to the states, but none have eliminated the basic rules of the realist game of survival, deterrence, power maximization, and competitive adaptation. The upcoming RMA V, which is largely based on the use of AI in C4ISR systems, information warfare, and cyber-enabled decision advantage, is going to be the same (Thiele, 2021: 68-70). The quick digitization and information orientation of Russia and China and the United States' attempt to keep up its technological advantage are classical Waltz's dynamics of balancing and arms racing under anarchy. The combination of information, surveillance, modelling, and AI-enabled targeting is also neoclassical in nature: states transform material technologies into strategic power via domestic institutions, industrial ecosystems, and elite threat perceptions. Furthermore, the conjunction of RMAs I–V, mostly by Russia and China, indicates that the hybrid warfare is not a new phenomenon but an evolutionary deepening of the psychological, coercive, and sub-conventional strategies with which classical realism has been familiar for a long time. Therefore, the RMA literature is a strong analytical backing to the argument that the integration of cyber, AI, and information tools in U.S. national security strategy is a move within existing realist traditions and not a break.

Realist logic in US Cyber-AI-Information Strategy

The research has used document analysis to get cognizance of the US strategy on hybrid warfare. US policy on security does not mention realism explicitly. But the language of the document very much indicates the realist logic. The DoD Cyber Strategy clearly shows a realist reasoning when it depicts the internet world as a new battlefield for the competition of the power. The department will face enemies that want to "erode U.S. military advantages," which is in line with the ideas that Waltz presents about anarchy and the security dilemma, where the worries about relative gains and military superiority are still the main ones. Their mantra of "deterring aggression," "defending forward," and "degrading adversary capabilities" is a telling sign of classical realist thoughts regarding power as the faculty to influence or limit the behavior of other actors. Along with that, the focus of the document on Defense Industrial Base, public-private partnership, and sophisticated institutional mechanisms is in agreement with neoclassical realism which assumes that domestic capacity and bureaucratic structures are the mediators that convert systemic pressures into a concrete strategy. In this way, the language and the issues highlighted in the DoD Cyber Strategy are a strong indication that the argument that U.S. cyber and information-domain integration is a continuation of realism rather than a theoretical rupture is valid.

Additionally, the DoD Cyber Strategy is also a reflection of a clearly realist perspective of threats. It does this by presenting cyberspace as the arena where the strategic competition is continuous whereas conflict is episodic. The document makes a point that adversaries like China and Russia perform "persistent engagement" in the area below the level of armed attack, this is a terminology that is very much in line with Mearsheimer's offensive realism that suggests that great powers always look for opportunities to increase their relative power in a situation that is uncertain (Mearsheimer 2001). The focus on resilience, supply-chain security, and the reviving of the Defense Industrial Base is, therefore, a reflection of neoclassical realist Rose's insight that states have to mobilize their internal resources if they are to respond to external pressures effectively (Rose 1998). In sum, these features point to the U.S. cyber posture as being theoretically based on realism's core assumptions: the centrality of power, the inevitability of competition, and the primacy of national security in an anarchic situation. Therefore, the cyber strategy is not a new paradigm but rather the evolution of the longstanding realist logic to the digital age.

Moreover, the realist logic of power to dominate finds glimpses in the statements of US officials. US secretary of state Macri Rubio, for instance, says that “winning AI race is non-negotiable. America must continue to be a dominant force in Artificial Intelligence to promote prosperity and protect our economic and national security”. The U.S. Department of State’s new Enterprise Data and AI Strategy is a clear example that the use of AI, data analytics, and other information-domain tools in American statecraft is not a break with traditional realism but rather a technological adaptation of it. The language of the document shows that it follows the logic of structural realism: AI is presented as a strategic resource that is necessary for maintaining “American leadership globally,” making “national security” stronger, and allowing quicker and more accurate "responses to geopolitical shifts" all these being very much in line with Waltz’s concerns about relative gains and systemic competition in an anarchic system. Moreover, the strategy’s focus on manipulating information environments, providing diplomats with predictive insights, and giving negotiators the possibility of “AI-powered analysis” is very much in line with Morgenthau’s classical realist view of political power as the ability to affect the minds and perceptions of others. The strategy also mirrors the primary assumptions of structural realism by presenting AI as a strategic resource indispensably needed for maintaining the US leadership role in the world, keeping relative advantages over rivals, and responding effectively to “geopolitical shifts” - all “systemic concerns rooted in anarchy”. The focus on ensuring secure technological infrastructure, speeding up capability development, and making AI an integral part of diplomatic statecraft shows that AI is seen as a new tool for the power struggle to continue, rather than a way out of it.

Case Studies

Methodologically, this paper has employed qualitative case study approach to see how U.S has dealt with cyber, A.I, and information in ways consistent with realism. By examining US responses, the study demonstrates how strategic logic of power maximization, threat perception, and security dilemma is manifested in hybrid threat environments.

To start with, Office of Personnel Management (OPM) data breach of 2015 becomes a peculiar case study to understand the intelligence warfare through cyber intrusion. The incident shows how adversaries have exploited vulnerabilities. The attackers installed PlugX malware on OPM computers using a fake McAfee file (mcutil. dll) and the communication was done through encrypted SSL channels. Usually, malicious code is hidden in normal network traffic but this time the hackers exploited system trust to do long-term espionage without any visible confrontation. The command-and-control servers looked like real ones (e.g., "opm-security.org") and had funny names like "Steve Rogers" and "Tony Stark". This points out how identity spoofing and psychological misdirection are used by hybrid threats, thus they can infiltrate persistently with very little suspicion. The sluggish response from OPM was due to the disorganized bureaucracy which included confusion between two similarly named cybersecurity vendors (Cylance and CyTech). Hybrid adversaries thus, directly gained from such structural vulnerabilities which eventually delayed their response and prolonged their time to exploit. The attackers by integrating the OPM systems with the hidden command-and-control channels have turned network-centric warfare on its head. The adversaries, instead of the U.S., who had the information dominance, are now the ones who control the flow of information showing that hybrid warfare eliminates the difference between the frontline and administrative networks. The OPM breach reveals the paradox of the U.S. national security system that is at once vulnerable and invulnerable. On the one hand, the U.S. has overall technological superiority but on the other hand systemic weaknesses such as outdated systems, security tools that are inconsistently adopted, and internal bureaucratic politics have created an entry point for hybrid adversaries that could be exploited. The attackers had far fewer resources than the defenders but were able to cause a strategically disproportionate impact. Later investigations also indicates that the malware was officially sponsored by Chinese government. The plug x installed at backdoor was associated with Chinese language hacking group (Fruhlinger, 2020).

Another case study of US CYBER COMMAND shows how U.S. operational doctrine (defend forward) has realist logic of preemption, deterrence, and balance of capabilities. The evolution of U.S. cyber strategy over a decade, markedly shows a transition from network-centric defense to outward-looking operational doctrine of defend forward and its partner strategy persistent engagement. Generally, the Department of Defense strategies that include the 2011 Strategy for Operating in Cyberspace were heavily reliant on "active cyber defense" which was mostly within the DoD networks themselves. What was new in the 2015 Cyber Strategy was the extension of the mandate to cover security of the civilian as well as the private sector networks during the time of tension (Kosseff 2019, pp. 3–4). The final stage was marked with the help of the 2018 U.S. Cyber Command's Command Vision which mentioned that "defending forward as close as possible to the origin of adversary activity" not only permits the United States to reveal the adversary capabilities but also "impose tactical friction and strategic costs" as a result of continuous engagement (U.S. Cyber Command, 2018 as cited in Kosseff, 2019 p. 5).

The public version of DoD Cyber Strategy (2018) was more elaborate in its presentation of Defend Forward as a way to "disrupt or halt malicious cyber activity at its source" fair enough to acknowledge operations in the gray area of armed conflict, thus signaling a move away from purely defensive reactive postures towards anticipatory, real-time disruption of adversary campaigns (Kosseff 2019 pp. 5–6). In accordance with this concept, USCYBERCOM has shifted its focus to forward positioning, better warning, and influence—to employees' advantage in the cyberspace of the enemy, early detection of threats, shaping adversary behavior, and sending a signal that hostile cyber activities will be responded to (Kosseff 2019 pp. 7–8). As per its official history, this change mirrors a more general transformation of USCYBERCOM from scattered task forces of yesteryear to a single unified combatant command capable of acting globally in real-time (U.S. Cyber Command, 2024). While on their own these developments demonstrate how cyber doctrine in the US revolves around the idea of cyberspace as a continuous battlespace, they also argue for the necessity of a proactive as well as a persistent strategy of engagement if national interests are to be effectively safeguarded.

Outcomes

The data obtained through this research strongly make the case for the hypothesis that the cyber and information operations domain strategy of the U.S. is essentially in line with the traditional realist strategic logic of the established branch rather than breaking away from theory. The text materials from which the analysis was done, i.e. the doctrinal documents, especially the DoD Cyber Strategy, used the words in a very consistent manner to present cyberspace as a natural follow-up to competition in the geopolitical arena, where relative power, military advantage, and the security dilemma are threatened. The employ of expressions like "eroding U.S. military advantages," "deterring aggression," and "defending forward" manifest an explicit allegiance to core and structural realist postulates regarding anarchy, competition, and the predominance of military capability.

Moreover, the examination of the OPM breach as a case further accentuates this point: the administration in Washington did not see the intrusion as a new type of war, but as a more complex version of a long-established pattern of spy activities, resulting in the choice of responses that are typical for a deterrence strategy, strengthening the target, and reorganizing intelligence.

Besides that, the study reveals the integration of neoclassical realist factors in the U.S. cyber strategy by giving prominence to domestic capacity, such as public-private partnerships, bureaucratic alignment, and the Defense Industrial Base, that are the main facilitators of systemic pressures.

Placed within the context of scholarly debates, the results of this study correspond to those of continuity theorists, i.e., Rid (2013), Nye (2010), and Edelman (2013), all of whom maintain that cyber operations are still deeply embedded in the traditions of statecraft and do not signify the occurrence of a "paradigm shift." Consequently, the amassed proof is indicative of the fact that the U.S. mixed warfare

stance, which comprises the cyber and information elements, should be perceived as the digital-age progression of the realist strategic logic of the core concept rather than as a break from it.

Is Realism still adequate?

Neo-liberal scholar Joseph Nye (2010) for instance disputed that "the characteristics of cyberspace reduce some of the power differentials among actors and thus provide a good example of the diffusion of power that typifies global politics in this century". He adds that "the low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace…than in many traditional domains". He is contesting the traditional realist logic of power, coercion, and deterrence which is inadequate in hybrid threats. For Nye, the power based on information resources is not new, but cyber power is present day phenomena (Nye 2010: 3-4). Nye's focus on the informational basis of power suggests, among other things, a move away of traditional deterrence toward more complex interactions that are interdependent and impacted by the speed of digital networks. This puts him in line with what scholars refer to as the "rupture thesis," which argues that cyber technologies change the fundamental way power is generated and used in world politics. By emphasizing how cyber weapons give power to non-state actors and make it difficult to attribute and retaliate against attacks, Nye is, in effect, saying that the virtual world offers control and disruption in ways that a realist theory, which is based on physical force and territoriality, cannot fully understand. Therefore, his argument positions cyber power not as a mere extension of classical military dominance but rather as a new qualitatively different space where traditional power logics are unsettled.

Another scholar, Mary Caldor (2012), writes that "The new type of warfare has to be understood in terms of global dislocation. New forms of power struggle may take the guise of traditional nationalism, tribalism or religious fundamentalism, but they are, nevertheless, contemporary phenomena arising from contemporary causes and displaying new characteristics." Kaldor considers hybrid warfare not only as a new tool used in old geopolitical contests but also as a different kind of violence that is influenced by globalization, weak governance, economic collapse, migration, and identity politics. The main means of power are no longer territorial conquest or military force but rather information manipulation, fear, identity mobilization, and social fragmentation. Her emphasis on identity politics and non-state actors additionally indicates that power in contemporary conflicts is spread out, deeply ingrained in society, and most of the time decentralized, therefore, it contradicts the realist assumption that states are the main and rational causes of war. Accordingly, Kaldor sees hybrid warfare as resulting from worldwide interconnectedness and local fragility, hence, she is pointing to those scare of violence which are indistinguishable from each other in terms of war and politics, state and non-state actors, as well as domestic and international arenas.

Conclusion

While scholars such as Nye and Kaldor argue that phenomena like cyber diffusion, identity-driven violence, and networked disruptions lessen the power of realism to explain these situations, the U.S. national security strategy evidence shows that hybrid threats are not beyond the red line of realist logic rather they intensify it. The digital world has not done away with power politics; it has simply moved them. Cyber capabilities, AI systems, data infrastructures, and information operations have become new tools through which the classical realist struggle for influence, prestige, and security is carried out.

The future international order will depend on the way major powers will use data, algorithms, and information flows as weapons to achieve their long-term goals of domination, deterrence, and survival. Hybrid threats may make the strategic environment more difficult, but in the end, they confirm the continued existence of realist patterns in an era when power is contested just as fiercely in networks and information systems as it used to be on land and sea.

References

Edelman, R. D. (2013). *Cyberattacks in international relations* (D.Phil. thesis, University College, University of Oxford, United Kingdom). Oxford University Research Archive.

Filipec, O. (2019). *Hybrid warfare: A critical perspective in the context of international relations theories*. Central European Journal of Politics, 5(2), 52–71.

Fruhlinger, J. (2020, February 12). *The OPM hack explained: Bad security practices meet China's Captain America.* CSO Online. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*.

Thiele, R. (Ed.). (2021). *Hybrid warfare: Future and technologies*. Springer Fachmedien Wiesbaden.

Kaldor, M. (2012). *New and old wars: Organized violence in a global era* (3rd ed.). Polity Press.

Kosseff, J. (2019). *The contours of "defend forward" under international law*. In T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, & G. Visky (Eds.), Silent Battle (pp. 1–15). NATO CCD COE Publications.

Morgenthau, H. J. (1949). *Politics among nations: The struggle for power and peace*. Alfred A. Knopf.

Nye, J. S., Jr. (2010, May). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

U.S. Department of Defense. (2018). *DoD cyber strategy* [Summary].

U.S. Cyber Command. (2024). *History of U.S. Cyber Command*. U.S. Department of Defense. https://www.cybercom.mil/About/History/

U.S. Department of State. (2025, September). *Enterprise data and artificial intelligence strategy* [PDF]. https://www.state.gov/wp-content/uploads/2025/09/Department-of-State-Enterprise-Data-and-AI-Strategy.pdf